AUSTRALIAN ENERGY MARKET COMMISSION

RULE

Consultation paper

Cyber security roles and responsibilities consultation paper

Proponent

The Honourable Chris Bowen, Minister for Climate Change and Energy

20 June 2024

Inquiries

Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

E aemc@aemc.gov.au
T (02) 8296 7800

Reference: ERC0388

About the AEMC

The AEMC reports to the energy ministers. We have two functions. We make and amend the national electricity, gas and energy retail rules and conduct independent reviews for the energy ministers.

Acknowledgement of Country

The AEMC acknowledges and shows respect for the traditional custodians of the many different lands across Australia on which we all live and work. We pay respect to all Elders past and present and the continuing connection of Aboriginal and Torres Strait Islander peoples to Country. The AEMC office is located on the land traditionally owned by the Gadigal people of the Eora nation.

Copyright

Citation

To cite this document, please use the following:
AEMC, Cyber security roles and responsibilities consultation paper, Consultation paper, 20 June 2024

Summary

1 Cyber security is a critical concern within Australia. While it impacts all sectors, the issue is especially prominent in the energy security space given the National Electricity Market's (NEM) increasing digitisation and connectivity. The integration of information and communications technology (ICT) and connectivity heightens the power system's cyber vulnerability. A cyber incident could have widespread and far-reaching implications.

2 In early 2024, the Australian Energy Market Commission (AEMC or the Commission) received a rule change request from The Honourable Chris Bowen, Minister for Climate Change and Energy. The rule change request seeks to confirm and clarify cyber security preparedness role and responsibilities that the Australian Energy Market Operator (AEMO) would perform to assist in protecting the energy system against cyber security incidents.

3 The proponent proposes that as energy systems become increasingly interconnected and reliant on digital technologies, the potential impact of a cyber breach amplifies. The proponent identifies two broad issues relating to the current cyber security arrangements in the National Electricity Rules (NER or the rules):

1. cyber security is not explicitly referenced in the rules as it relates to power system security
2. specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the energy system are not specified in the rules.

4 The AEMC has commenced its consideration of the request and this consultation paper is the first stage.

The rule change request identifies issues with the lack of explicit references to cyber security in the current NER

5 We are seeking stakeholder views on the following issues raised in the rule change request.

6 The rule change proponent considers there is a need to confirm and clarify AEMO's role and responsibilities for cyber security in the National Electricity Rules (NER).

7 Confirming and clarifying AEMO's role and responsibilities would provide:

1. funding certainty for AEMO to fulfil the specific identified functions in the rules required to maintain and improve power system cyber security
2. clarity in the rules and clear guidance, leadership, or accountability with respect to the specific identified functions in the rules required to improve cyber security.

8 The proponent considers that the lack of funding certainty and liability protection for the delivery of these additional functions has led to AEMO performing these services without sufficient resources. The proponent considers that this lack of consistency has the potential to harm the power system, since it could weaken the management of cyber risks across the power system.

9 While not specifically referenced, AEMO's existing statutory function under the National Electricity Law (NEL) to "maintain and improve power system security" inherently extends to cyber incidents impacting power system security In this context, the NER further references AEMO's authority to issue power system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment.

10 For this reason the proponent considers that confirming AEMO's cyber security functions in the NER would provide sufficient clarity on its role and responsibility. We are seeking stakeholder

feedback on whether including these additional functions in the rules would benefit both industry and government by providing clarity in what to expect from AEMO regarding cyber security.

The request seeks to establish cyber security as a function in the NER

11 We are also seeking stakeholder views on the solutions proposed in the rule change request, which consist of:

1. explicitly referencing cyber security in theNER as they relate to power system security
2. Including four additional cyber security functions in the rules to ensure a strategic and coordinated approach to cyber security.

12 The proponent considers that the ad hoc nature of AEMO's engagement and lack of resourcing poses an ongoing risk to the security of the NEM. To resolve this, it seeks to:

1. clarify cyber security as a function within AEMO's existing role to maintain power system security which would enable AEMO to recover costs for these services and confirm AEMO's immunity from liability for the delivery of these services.
2. establish a coordinated and strategic approach to manage the increasing cyber security risk to the power system by outlining a set of four new functions for cyber security for AEMO within the broader context of power system security.

13 Importantly, the proponent proposes that these four new functions in the rules would be facilitative and **would not of themselves provide AEMO with the ability to impose mandatory obligations on participants.** The request also notes that NEM participants would retain sole responsibility and agency for ensuring their own cyber security needs are met.

14 **Function 1: Cyber security incident coordinator**. As cyber security incident coordinator, AEMO would be able to plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. The proponent suggests that AEMO could develop a plan outlining how market, state, and federal responses to a cyber incident would be coordinated. The proponent refers to this as the Australian Energy Sector Cyber Incident Response Plan (AESCIRP). In the event of a cyber incident, AEMO would lead the implementation of the response in the manner set out by the plan.

15 **Function 2: Supporting cyber preparedness and uplift.** This could include:

- **Stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF)**[1] | AEMO previously played a role in developing the AESCSF and they would continue to be involved in updating and maintaining the framework. This function could also include administering AESCSF self-assessments for the energy industry. Note that AEMO already carries out this work, but the proponent would provide ongoing resourcing certainty.
- **Organisation of testing and training exercises** | As part of this function, AEMO could support or undertake the development and delivery of scenario exercises to test the cyber resilience of the power system and industry participants.
- **Provision of guidance and advice to industry** | As part of this function, AEMO could provide industry cyber security guidance in the form of written materials, digital tools, participation in working groups, or by other means. The proponent notes that it does not intend for AEMO to create additional mandatory guidelines on cyber security.

16 **Function 3: Examining risks and providing advice to government and industry.** This function

1 The AESCSF program provides a tool for assessing cyber security maturity across Australia's energy sector. It was developed through collaboration with industry and government.

would involve AEMO providing cyber security research and advice to governments on request. This advice would draw on AEMO's unique energy expertise in their position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre (ACSC).

17 **Function 4: Facilitating the distribution of critical cyber security information to market participants.** In this function, AEMO would act as a distributor of cyber security information to the energy industry, using their position as system operator and existing communication channels. AEMO could facilitate the distribution of information including, but not limited to:

- warnings of cyber vulnerabilities or threats
- annual AESCSF assessment conclusions
- post-cyber incident reports
- preventative patches in commonly used technologies.

18 The proponent notes that the estimated cost increase to do all four functions would be less than $10 million per year, which is an increase of two per cent of AEMO's total participant fees. This would be on an ongoing basis, but the proponent considers that this is an estimate and the ongoing cost may change depending on the evolving cyber threat landscape and the resources required by AEMO to manage new and emerging threats accordingly over time.

We consider that there are three assessment criteria that are most relevant to this rule change request

19 Considering the NEO[2] and the issues raised in the rule change request, the Commission proposes to assess the rule change request against the following three assessment criteria.

- **Safety, security and reliability:** safety and security outcomes for consumers are the end goal of the proposed rule change. Cyber security incidents present an energy sector risk that could have significant consumer impacts. The proposal seeks to clarify AEMO's functions regarding cyber security, which could help enable the secure provision of electricity to end customers over the long term.
- **Principles of good regulatory practice:** principles of good regulatory practice will be critical to this rule change request. This is because the rule change proposal seeks to improve predictability, stability and transparency without being overly prescriptive. Further, this rule change request will need to consider the broader direction of cyber security reforms to avoid duplication.
- **Implementation considerations:** implementation considerations will be critical to developing a good solution for this rule change request. Implementation issues cover cost implications and timing considerations as well as understanding any relevant jurisdictional conditions and if there are material implementation issues affecting industry participants.

20 These criteria and their selection process are explained in detail in section 4.2.

Full list of consultation questions

2 Section 7 of the NEL.

Question 1: Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?

Question 2: Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?

Question 3: Would the industry value more cyber security guidance in the NER, why/why not? If yes, what kind of guidance specifically?

Question 4: Do you agree that the lack of clarity regarding the identified cyber security functions in the rules is problematic? Why or why not?

Question 5: Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither? Why/why not?

Question 6: Do you consider that the benefits for clarifying the cyber security incident coordinator as a function for AEMO in the rules outweigh the costs/risks? Why/why not?

Question 7: Do you consider clarifying the supporting cyber preparedness and uplift as afunction in the rules outweigh the costs/risks? Why/why not?

Question 8: Do you consider the benefits of clarifying the examining risks and providing advice to government and industry as a function in the rules outweigh the costs/risks? Why/why not?

Question 9: Do you consider the benefits of claryfing the facilitating the distribution of cyber security information to market participants as a function in the rules outweigh the costs/risks? Why/why not?

Question 10: Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?

How to make a submission

We encourage you to make a submission

Stakeholders can help shape the solutions by participating in the rule change process. Engaging with stakeholders helps us understand the potential impacts of our decisions and, in so doing, contributes to well-informed, high quality rule changes.

We have included questions in each chapter to guide feedback, and the full list of questions is above. However, you are welcome to provide feedback on any additional matters that may assist the Commission in making its decision.

Submissions are due Thursday 18 July with other engagement opportunities to follow

Due date: Written submissions responding to this consultation paper must be lodged with Commission by **Thursday, 18 July 2024.**

How to make a submission: Go to the Commission's website, www.aemc.gov.au, find the "lodge a submission" function under the "Contact Us" tab, and select the project reference code ERC0388.[3]

You may, but are not required to, use the stakeholder submission form published with this consultation paper.

Tips for making submissions are available on our website.[4]

Publication: The Commission publishes submissions on its website. However, we will not publish parts of a submission that we agree are confidential, or that we consider inappropriate (for example offensive or defamatory content, or content that is likely to infringe intellectual property rights).[5]

Other opportunities for engagement

There are other opportunities for you to engage with us, such as one-on-one discussions or industry briefing sessions. See below for instructions and contact details for the project leader.

For more information, you can contact us

Please contact the project leader with questions or feedback at any stage.

Project leader:	Nomiky Panayiotakis
Email:	nomiky.panayiotakis@aemc.gov.au
Telephone:	(02) 8296 7810

3 If you are not able to lodge a submission online, please contact us and we will provide instructions for alternative methods to lodge the submission.

4 See: https://www.aemc.gov.au/our-work/changing-energy-rules-unique-process/making-rule-change-request/submission-tips

5 Further information is available here: https://www.aemc.gov.au/contact-us/lodge-submission

Contents

Tables

1 The context for this rule change request

In early 2024, the Australian Energy Market Commission (AEMC or the Commission) received a rule change request from The Honourable Chris Bowen, Minister for Climate Change and Energy. The rule change request seeks to confirm and clarify the cyber security preparedness roles and responsibilities to be performed by AEMO to assist in protecting the energy system against cyber security incidents.

This section provides an overview of Minister Bowen's rule change request along with relevant context and background.

This section sets out:

- Section 1.1 — Cyber security is a growing and prevalent issue
- Section 1.2 — This rule change proponent proposes to clarify AEMO's role in cyber security
- Section 1.3 — Cyber security governance has expanded within the last ten years
- Section 1.4 — We have started the rule change process.

1.1 Cyber security is a growing and prevalent issue

Cyber security is a critical concern within Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the National Electricity Market's (NEM) increasing digitisation and connectivity. This includes real-time data of critical power system components, supervisory control and data acquisition (SCADA) systems, smart grids, smart meters and smart appliances connected to open networks. Additionally, the NEM's high uptake of Consumer Energy Resources (CER) and distributed energy resources (DER) such as neighbourhood batteries further amplifies the issue

Digitisation can bring a range of benefits including new opportunities for innovation and an increase in transparency at both a system-wide level and on an individual customer basis. Australia's high CER uptake also provides benefits including supporting a reduction in overall system costs, improving reliability, and achieving a secure, low-emission energy supply for all consumers.

However, the NEM's integration of information and communications technology (ICT) and connectivity also increases the power system's cyber vulnerability. The Australian Government defines cyber security as measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.[6] A cyber security incident in the electricity sector could have far-reaching implications, from widespread outages, to economic disruptions, breach of sensitive data and threats to national security. While the benefits of increased digitisation and connectivity are worth pursuing, it also requires enhanced capabilities to mitigate threats from any malicious cyber activity.

The cyber attack in Ukraine in December 2015 is the most well-known cyber security incident on a large energy grid. The attack on three regional electricity distribution companies impacted 225,000 customers.[7] Restoration efforts were delayed as the attack disabled control systems, disrupted communications and prevented automated system recovery.

6 Australian Cyber Security Centre, cyber.gov.au, 'Glossary'.
7 US Department of Homeland Security, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

While there has been no publicly reported large-scale cyber attack on Australia's power system, there has been a growing number of incidents on major corporations. Latitude, an Australian financial service provider, was breached in March 2023 which affected over 14 million individuals from Australia and New Zealand. The previous year, Australia also saw cyber attacks on Medibank and Optus. Each attack impacted just under 10 million customers, nearly 40 per cent of the Australian population. Both companies saw personal data compromised and Optus also experienced a widespread telecommunication outage. These incidents highlight the growing prevalence of cyber security in the Australian context.

1.2 Cyber security governance has expanded within the last ten years

Cyber security governance in Australia, particularly within the energy sector, has evolved over the past decade. One of the key milestones in the history of cyber security governance in Australia was the establishment of the Australian Cyber Security Centre (ACSC) in 2014. The ACSC serves as the central hub for cyber security coordination and information sharing between government, industry, and academia. It plays a crucial role in helping organisations within the electricity sector to enhance their cyber security posture and respond effectively to cyber incidents.

Later the Finkel Review, commissioned in response to the 2016 South Australian blackout, emphasised the importance of cyber security within the energy sector. Its recommendations underscored the necessity for resilient and secure energy infrastructure, with the report noting "strong cyber security measures for the NEM will be essential for maintaining Australia's growth and prosperity in an increasingly global economy."[8] The review recommended:[9]

> an annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board, in consultation with the Australian Cyber Security Centre and the Secretary of the Commonwealth Department of the Environment and Energy.

Building upon this recommendation, the Australian Energy Sector Cyber Security Framework (AESCSF) was developed as a framework to assess cyber security maturity across Australia's energy sector. It was developed through collaboration with industry and government stakeholders, including AEMO, ASCS, Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations. It is both a framework and an annual voluntary assessment program, enabling participants to undertake assessments of their own cyber security capability and maturity. Participants can use the results to inform and prioritise investment to improve cyber security posture.

In addition, the amended Security of Critical Infrastructure Act 2018 (the SOCI Act) expanded its scope to encompass the energy sector, acknowledging its vital role in national security. This legislative update mandated rigorous cyber security standards and incident reporting requirements for energy providers, elevating the industry's cyber security posture to align with contemporary threats. It outlines the legal obligations you have if you own, operate, or have direct interests in critical infrastructure assets. The SOCI Act also outlines how the government can support you if an incident occurs that impacts your critical infrastructure asset. As per the amended SOCI Act, it is AEMO's primary responsibility to maintain the cyber security of its own assets.

8 https://www.dcceew.gov.au/sites/default/files/documents/independent-review-future-nem-blueprint-for-the-future-2017.pdf, p. 67.
9 https://www.dcceew.gov.au/sites/default/files/documents/independent-review-future-nem-blueprint-for-the-future-2017.pdf, p. 69.

Table 1.1: Australian government bodies playing a role in cyber security

Body name	Description
Australian Signals Directorate (ASD)	A statutory agency within the Defence Portfolio which collects and communicates foreign signals intelligence, provides cyber security advice, and aims to protect Australia from cyber threats.
Australian Cyber Security Centre (ACSC)	An agency of the ASD which acts as the federal government's technical authority on cyber security, providing materials and advice for consumers, small and large businesses, and government.
Department of Home Affairs	Among other functions: • Supports the development and implementation of national cyber security policy. • Manages all types of threats to critical infrastructure, in partnership with industry and the broader community, through the CISC.
Cyber and Infrastructure Security Centre (CISC)	Assists critical infrastructure owners and operators to understand risk and meet regulatory requirements. Reports to the Department of Home Affairs.
State and territory cyber security units	The larger jurisdictions have cyber security units that support government (and sometimes public sector) cyber security initiatives. They may also be responsible for leading jurisdictional government responses to cyber incidents. Smaller jurisdictions usually fulfil this function within an existing department.

Source: ASD; ACSC; Department of Home Affairs - 'Cyber security', 'Critical infrastructure security'; CISC; QLD Government - 'About the Cyber Security Unit'; NSW Government - 'Cyber Security NSW'; VIC Government - 'About the Cyber Security Unit'; Government of WA - 'Cyber Security Unit'.

As noted above, the recently amended SOCI Act places cyber security obligations on owners and operators of critical infrastructure, including electricity and gas infrastructure.[10] The AESCSF can be used by owners and operators to meet SOCI Act requirements.[11] Aside from this, the Commission is not aware of any other Australian policy or regulations on cyber security specifically for the energy sector. The SOCI Act effectively requires NEM participants, including AEMO, to manage their own critical infrastructure in a cyber secure manner, whereas this rule change is primarily concerned with facilitating cohesive cyber security practices across all NEM participants.

One such practice mentioned in the rule change request is a cyber incident response plan for the energy sector.[12] Each NEM state or territory has an emergency management plan developed by a government agency that would apply in a significant cyber or energy supply incidents.[13] Many

10 Australian Government, https://www.legislation.gov.au/C2018A00029/latest/text.

11 AEMO, https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.

12 Rule change request to the AEMC, Minister Bowen, p. 4.

13 NSW Government, https://www.nsw.gov.au/rescue-and-emergency-management/state-emergency-management-plan-emplan;
Emergency Management Victoria, https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-semp;
Queensland Government Disaster Management, https://www.disaster.qld.gov.au/plans;
Government of South Australia Department of the Premier and Cabinet, https://www.dpc.sa.gov.au/responsibilities/security-emergency-and-recovery-management/state-emergency-management-plan;
TAS State Emergency Service, https://www.ses.tas.gov.au/emergency-management-2/tasmanian-emergency-management-arrangements-tema/;

states also have specialised sub-plans for a loss of electricity supply or a potential severe energy shortage, but they do not specifically consider cyber events as a potential cause of such emergencies.[14] Similarly, many jurisdictions have a sub-plan for a serious cyber incident, but these do not consider a cyber incident impacting the energy sector specifically. This means there may be a need for a bespoke NEM cyber incident response plan.

While the scope of this rule change is the NEM - governed by the NER - there may be a similar need to confirm and clarify functions in other Australian energy systems. Like the NER, the National Gas Rules (NGR) cover system security in a general sense but do not include cyber security provisions.[15] The situation is similar for the Wholesale Energy Market (WEM) Rules which apply to the Western Australian electricity system.[16] The rule change proponent states they will look to address cyber security in the WEM and gas markets through separate processes.[17]

1.3 This rule change proponent proposes to clarify AEMO's role in cyber security

The proponent proposes that as energy systems become increasingly interconnected and reliant on digital technologies, the potential impact of a cyber breach amplifies and underscores the urgent need for robust and clearly defined security measures and roles, to support vigilance within the energy space.

The proponent identifies two broad issues relating to the current cyber security arrangements in the National Electricity Rules (NER or the rules):

1. cyber security is not explicitly referenced in the rules, as it relates to power system security
2. specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the energy system are not specified in the rules.

The proponent considers that the ad hoc nature of AEMO's engagement and lack of resourcing for these additional functions in the NER poses an ongoing risk to the security of the NEM. To resolve this, it seeks to clarify cyber security as a function within AEMO's existing role to maintain power system security and add four new preventative functions for AEMO in the NER to perform to assist to maintain a secure power system. While AEMO has performed some of these functions (see chapter 2), the request considers that this has been done so in a limited capacity using existing resources. These changes would enable AEMO to recover the costs it incurs in carrying out these functions and confirm AEMO's immunity from liability for the delivery of these functions.

The rule change request can be found on the project page: https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities.

1.4 We have started the rule change process

This paper is the first stage of our consultation process. The Commission invites stakeholders to make submissions on the stated problem and the proposed solutions.

We are using the standard rule change request process, which includes the following formal stages:

ACT Emergency Services Agency, https://esa.act.gov.au/be-emergency-ready/emergency-arrangements.

14 'Sub plan' is the term used for a hazard-specific plan which is subordinate to the overall emergency management plan, and details the arrangements for preventing, preparing for, and responding to an emergency of that type.

15 AEMC, National Gas Rules, https://energy-rules.aemc.gov.au/ngr/558.

16 Government of Western Australia, WEM Rules, https://www.wa.gov.au/government/document-collections/wholesale-electricity-market-rules.

17 Rule change request to the AEMC, Minister Bowen, p. 4.

- a proponent submits a rule change request
- the Commission commences the rule change process by publishing a consultation paper and seeking stakeholder feedback
- stakeholders lodge submissions on the consultation paper and engage through other channels to make their views known to the AEMC project team
- the Commission publishes a draft determination and draft rule (if relevant)
- stakeholders lodge submissions on the draft determination and engage through other channels to make their views known to the AEMC project team
- the Commission publishes a final determination and final rule (if relevant).

The key dates for this process are outlined in Table 1.1 below.

Table 1.2: Key project dates

Milestone	Key dates
Publication of consultation paper	20 June 2024
Close of submissions to the consultation paper	18 July 2024
Publication of draft determination (and draft rule)	26 September 2024
Publication of final determination (and final rule)	19 December 2024

Information on how to provide your submission and other opportunities for engagement is set out at the front of this document .

You can find more information on the rule change process on our website.[18]

18 See our website: https://www.aemc.gov.au/our-work/changing-energy-rules.

2 The problem raised in the rule change request

This chapter seeks stakeholder feedback on the problem identified in the rule change request — whether it is or will soon become a problem and if so, the scale and impact of the problem.

The rule change request, submitted by The Honourable Chris Bowen, Minister for Climate Change and Energy, notes that currently, AEMO's role in cyber security is less well understood when compared to its traditional role in maintaining a secure technical envelope. The request further suggests that a coordinated and strategic approach is needed to effectively manage the increasing cyber security risk to power system security.

This section summarises the issues raised in the rule change request including:

- Section 2.1 — Cyber security activities are undertaken on an ad hoc basis
- Section 2.2 — Cyber security is not explicitly referenced in the rules.

2.1 Issue 1 — Cyber security activities are undertaken on an ad hoc basis

The proponent considers that there is currently a need to confirm and clarify, in the NER, what AEMO's preventative role and responsibilities are in relation to cyber security.

The proponent considers that:[19]

> NEM participants, government and AEMO would benefit from greater clarity within the legislative framework, acknowledging the overlap between the activities to improve and maintain power system security and cyber security management (i.e., emergency management arrangements) and the breadth of activities this could include. Without a clear allocation of agreed responsibility ownership and accountability across government and industry, cyber security efforts and capability to respond to incidents will be impacted.

The proponent further notes that AEMO is concerned the current NEL and NER:[20]

> do not provide protection from liability or enable cost recovery. Clarifying AEMO's cyber security role will alleviate this concern.

To alleviate this concern, the proponent proposes that four additional functions be outlined in the NER to clarify AEMO's role in cyber security. These functions are outlined in section 3.2.

Question 1: Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?

2.1.1 AEMO currently lacks funding certainty to undertake the four additional cyber security roles and responsibilities outlined in the rule change request

The proponent notes that without an explicit reference to AEMO's additional role and responsibilities for cyber security to be performed by AEMO within the NER, AEMO is unable to recover fees for these services or receive protection from liability when performing these services.

19 Rule change request to the AEMC, Minister Bowen, p. 3.
20 Rule change request to the AEMC, Minister Bowen, p. 6.

The proponent considers that the lack of funding certainty and liability protection for the delivery of these services has led to AEMO performing these functions on an ad hoc basis, without sufficient resources. The lack of consistency has the potential to harm the power system, as the proponent considers it weakens the management of cyber risks across the power system, noting:[21]

> The ad hoc nature of AEMO's engagement and lack of dedicated resourcing for the activities described above poses an ongoing risk to NEM security. As time passes without sufficient action, the risk will increase and the ability of AEMO, government and industry to curtail these risks will become more challenging.

2.1.2 The energy industry lacks guidance or central orchestration

As outlined in section 1.2, cyber security governance of the power system has evolved within the last decade. This has resulted in legislative structures being developed at the federal level, including the SOCI Act 2018, as well as cross-organisational frameworks such as the Australian Energy Sector Cyber Security Framework (AESCSF).

However, the proponent considers that cyber security threats and AEMO's proposed responsibilities and actions in this area are unclear. This compares to more traditional power system security threats which are better understood by stakeholders. The proponent considers that greater clarity on the additional roles and responsibilities of cyber security is needed in the NER, noting:

> NEM participants, government and AEMO would benefit from greater clarity within the legislative framework, acknowledging the overlap between the activities to improve and maintain power system security and cyber security management (i.e., emergency management arrangements) and the breadth of activities this could include. Without a clear allocation of agreed responsibility ownership and accountability across government and industry, cyber security efforts and capability to respond to incidents will be impacted.

Overlapping or absence of clear policies within cyber security could create confusion and inefficiencies. There is also the risk of inconsistent implementation and falling short of cyber security standards. The Commission is seeking feedback on whether stakeholders consider there is currently a lack of policy guidance in the cyber security space related to the energy sector.

Question 2: Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?

Question 3: Would the industry value more cyber security guidance in the NER, why/why not? If yes, what kind of guidance specifically?

21 Rule change request to the AEMC, Minister Bowen, pp. 6-7.

2.2 Issue 2 — AEMO's cyber security role is not specifically defined in the rules

In addition to a lack of clarity on what the specific responsibilities are for AEMO with respect to cyber security, the proponent also considers that cyber security should be added as a function in the NER. The need for explicit references to cyber security was not envisioned at the time of the NEM's creation, given that cyber security was not a historically prevalent issue.

However, in the last ten to 15 years, the increasing digitisation of the NEM means that cyber security is now inextricably linked with the management of the energy market and systems. The proponent considers that understanding of AEMO's role in maintaining a secure power system with respect to cyber security has not kept up with the increasing threat. It considers that:[22]

> AEMO's role and responsibility with respect to more traditional threats to power system security is well understood and accepted by industry and government. The quickly evolving and unconventional threat posed by cyber security means AEMO's obligations for cyber security, as part of its mandate to improve and maintain power system security, is less well understood.

AEMO's existing statutory function under the NEL to "maintain and improve power system security" extends to cyber security incidents impacting power system security. This includes AEMO's authority to issue system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment.

Question 4: Do you agree that the lack of clarity regarding the identified cyber security functions in the rules is problematic? Why or why not?

22 Rule change request to the AEMC, Minister Bowen, p. 2.

3 The proposed solution and implementation

The rule change proponent proposes to explicitly reference cyber security within the NER and to clarify AEMO's role in relation to cyber security threats and coordinating the response to any cyber security incidents by adding four new functions in the rules. The proponent proposes to do this by adding cyber security as a function in the NER, which would identify cyber security as a statutory function for the purpose of the NEL, enabling AEMO to recover fees and charges, and confirm AEMO's immunity from liability for the delivery of these services.

For the purposes of facilitating stakeholder consultation, we have grouped the proposed changes into two broad categories that relate to the two key issues identified in the rule change request:

- Section 3.1 — Change 1: Cyber security be explicitly referenced in the rules
- Section 3.2 — Change 2: A strategic and coordinated approach to cyber security

3.1 Change 1: Cyber security be explicitly referenced in the rules

The rule change proponent seeks to clarify that the additional cyber security activities identified to be set out in the rules are part of AEMO's broader mandate to maintain and improve power system security. We are interested in stakeholder feedback on the proposed solution.

The proponent considers that the lack of explicit references to cyber security is an oversight in the current NER and that defining AEMO's role in cyber security would:[23]

> give industry and government confidence in what to expect from AEMO in terms of supporting cyber security uplift and responding to cyber incidents or vulnerabilities which have the potential to impact energy supply.

The Commission is interested in stakeholder feedback on whether explicitly referencing these additional cyber security functions within the NER would provide greater clarity to participants of AEMO's role in maintaining and improving cyber security preparedness within the power system, in addition to other power system security needs.

Solution 1a: Cyber security be defined as a power system security issue

Specifically, the proponent considers that NER clause 4.3 that describes AEMO's power system security responsibilities be expanded to include a reference in general terms to AEMO's responsibilities with respect to cyber security and that a new sub-clause be added to set out those responsibilities in more detail (this is discussed further below in section 3.2).

The rule change proponent considers that this drafting could be achieved by inserting a new paragraph (c1) in clause 4.3.1 that notes:

- (c1) to coordinate and support cyber preparedness, response and recovery in accordance with *AEMO's cyber security functions*

Solution 1b: Cyber security be included as part of network planning and expansion

The proponent proposes that a possible alternative location to outline these cyber security functions in the NER is Part D of Chapter 5, which deals with network planning and expansion and includes (in rule 5.20A) a requirement for AEMO to undertake periodic general power system risk reviews.

23 Rule change request to the AEMC, Minister Bowen, p. 3.

However, the proponent's preferred location is Chapter 4 as it considers that 'power system security' better meets the nature of cyber security functions.

Question 5: Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither? Why/why not?

3.2 Change 2: A strategic and coordinated approach to cyber security

As discussed in chapter 2, the proponent considers that the current ad hoc nature of cyber security activities is increasing the risk of an incident on the power system. To resolve this problem, the rule change seeks to establish a coordinated and strategic approach to manage the increasing cyber security risk to the power system. Specifically, it seeks to establish a set of four new functions for cyber security for AEMO within the broader context of power system security. The proponent considered this would:[24]

> ensure AEMO has clear authority to deliver these functions and is resourced to support mitigation and management of cyber security risks in the markets it manages. It will also give industry and government confidence in what to expect from AEMO in terms of supporting cyber security uplift and responding to cyber incidents or vulnerabilities which have the potential to impact energy supply.

The proponent notes that while AEMO already performs some of these activities, to date it has done so on an as-needed basis and in a limited capacity using existing resources and through alternative arrangements. Codifying these functions in the rules would allow AEMO to be sufficiently resourced for delivering these functions and extend its protection from liability when it delivers these functions. This would support a broader uplift of cyber security maturity in the power system, helping to prevent a widespread cyber incident.

The functions would be flexible and would not enable AEMO to impose any additional mandatory obligations on participants

Importantly, the rule change proponent proposes that these additional functions set out in the NER would be facilitative and would not enable AEMO to impose any mandatory obligations on participants. Furthermore, NEM participants would retain sole responsibility and agency for ensuring their own cyber security needs are met. The proponent notes:[25]

> While AEMO should have an expanded role to support uplift of cyber security, its role will not extend to directly managing the cyber preparedness, response or recovery outside of AEMO's own technology networks and systems. Primary responsibility for managing cyber security remains with businesses and market participants, with policy leadership provided by cyber and security agencies at all levels of government.

The functions proposed have been designed to be flexible and to adapt as the needs of the system evolves and technology continues to advance. In addition, the functions also seek to remain flexible within the existing legislation. The proposed changes would not seek to limit AEMO's existing functions that may be relevant to cyber security. The proponent also notes that

24 Rule change request to the AEMC, Minister Bowen, pp. 2 - 3.
25 Rule change request to the AEMC, Minister Bowen, p. 8.

there is no intention to impact the regulating roles of the Australian Energy Regulator, or the Department of Home Affairs in relation to the SOCI Act 2018.

The cost would be an increase of two percent in participant fees each year

As noted in section 2.1.1, this rule change request seeks to increase funding certainty for AEMO's role to perform the identified role and responsibilities set out in the NER in relation to cyber security. Cyber security is not a one-time investment but rather an ongoing process that requires continuous monitoring, adaptation, and innovation to stay ahead of malicious actors.

Box 1: How AEMO recovers fees from participants

AEMO recovers its costs from industry participants based on the extent to which participants are involved in AEMO's activities, through 'participant fees'. Participant fees include the recovery of various expenses, including those related to the operation of the national electricity market, power system security and reliability, major reform initiatives, and incremental services. These fees also cover a number of functions (or services) that AEMO performs to support the core operation of the NEM, including:

- national transmission planning (NTP)
- management of five-minute settlements (5MS)
- trading in the Settlements Residue Auction (SRA)
- management of the NEM2025 Reform Program
- facilitation of retail market competition
- provision of a consumer data platform
- integrating Distributed Energy Resources (DER) into the NEM.

Under section 119 in the NEL, prescribing functions such as these within the NER provides AEMO immunity from liability for the delivery of these services.

To ensure transparency, under the NEM, each year AEMO must publish:

- an annual budget of its revenue requirements by the start of each financial year
- a structure setting out how its budgeted revenue is to be recovered through participant fees.

For more information on AEMO's budget see: https://aemo.com.au/-/media/files/about_aemo/corporate-plan/2023/corporate-plan-2024-final.

The proponent notes that the estimated cost increase would be less than $10 million per year, which is an increase of two percent of AEMO's participant fees.[26] As outlined in Table 3.1, these costs would allow AEMO to perform the functions required to maintain and improve cyber security.

A breakdown of these costs are as follows:

Table 3.1: Expected costs

	Establishment	Y1	Y2	Ongoing
Cyber incident coordination	$4,525,000	$4,250,000	$3,150,000	$3,125,000
Coordination of	$0	$775,000	$400,000	$400,000

26 Specifically, the NEM core and NEM function segments which were roughly $319m in FY24.

	Establishment	Y1	Y2	Ongoing
cyber security research and advice				
Uplift of cyber security	$1,560,000	$2,025,000	$1,525,000	$1,525,000
Cyber security dissemination	$375,000	$350,000	$350,000	$350,000
Total costs	**$6,460,000**	**$7,400,000**	**$5,425,000**	**$5,400,000**

Source: Minister Bowen, rule change request

The proponent notes that the above are the expected costs and that the ongoing cost may change depending on the evolving cyber threat landscape and the resources required by AEMO to manage new and emerging threats accordingly over time. However, ensuring funding certainty would provide stability and predictability to the industry. It would allow these specific functions to be sufficiently resourced and could, for example, enable long-term initiatives, investment in essential resources and upskill personnel. Specifically, the proponent considers that:[27]

> Incorporating the proposed specific cyber security functions in the NER would provide AEMO, market participants and government confidence, that AEMO will deliver these functions on a consistent basis as part of its power system security responsibilities. Defining these roles will also reinforce the need for ongoing management of cyber risks and the need for strong collaboration with stakeholders to secure the markets AEMO operates.

3.2.1 Function 1: Cyber security incident coordinator

As cyber security incident coordinator, AEMO would be able to plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. The proponent suggests that AEMO could develop a plan outlining how market, state and federal responses to a cyber incident would be coordinated. The proponent refers to this as the Australian Energy Sector Cyber Incident Response Plan (AESCIRP). In the event of a cyber incident, AEMO would lead the implementation of the response in the manner set out by the plan.

The proposed rule change is designed to ensure resourcing and protection from liability for AEMO to perform this coordinator function. It would not give AEMO the ability to manage market participants' or other bodies' responses to a cyber incident.

Question 6: Do you consider that the benefits for clarifying the cyber security incident coordinator as a function for AEMO in the rules outweigh the costs/risks? Why/why not?

3.2.2 Function 2: Supporting cyber preparedness and uplift

The function of supporting cyber preparedness and uplift for the energy industry could include, but would not be limited to, the following:

- **Stewardship of the AESCSF** | AEMO previously played a role in developing the AESCSF and they would continue to be involved in updating and maintaining the framework. This function

27 Rule change request to the AEMC, Minister Bowen, p. 7.

could also include administering AESCSF self-assessments for industry. Note that AEMO already carries out this work, but the rule change would provide ongoing resourcing certainty.

- **Organisation of testing and training exercises** | As part of this function, AEMO could support or undertake the development and delivery of scenario exercises to test the cyber resilience of the power system and industry participants.
- **Provision of guidance and advice to industry** | As part of this function, AEMO could provide industry cyber security guidance in the form of written materials, digital tools, participation in working groups, or by other means. The rule change proposal does not intend for AEMO to create additional mandatory guidelines on cyber security.

Question 7: Do you consider clarifying the supporting cyber preparedness and uplift as afunction in the rules outweigh the costs/risks? Why/why not?

3.2.3 Function 3: Examining risks and providing advice to government and industry

This function would involve AEMO providing cyber security research and advice to governments on request. This advice would draw on AEMO's unique energy expertise in their position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the ACSC. Governments could request, for example, AEMO's insight, analysis or risk management planning advice on the risks that cyber events may pose to the electricity industry. Such advice could take the form of the written reports which may or may not be made publicly available. The intention is that AEMO would be obliged to prepare advice as requested by a relevant Minister, subject to consultation on the nature of the research or advice, the cost of preparing it, and AEMO's capacity to do so.

As part of this function, AEMO could also, at its discretion, provide similar advice to NEM registered participants. The proponent considers the function should also include AEMO's maintenance and further development of the AESCSF.

The function would be advisory only and would not expand AEMO's regulatory responsibilities, nor affect the roles of other regulatory or government bodies. Advice and risk evaluation provided under this function would be separate to AEMO's responsibilities under the General Power System Risk Review.

Question 8: Do you consider the benefits of clarifying the examining risks and providing advice to government and industry as a function in the rules outweigh the costs/risks? Why/why not?

3.2.4 Function 4: Facilitating the distribution of critical cyber security information to market participants

In this function, AEMO would act as a distributor of cyber security information to the energy industry, using their position as system operator and existing communication channels. AEMO could facilitate the distribution of information including, but not limited to:

- warnings of cyber vulnerabilities or threats
- annual AESCSF assessment conclusions
- post-cyber incident reports

- preventative patches in commonly used technologies.

The information distribution function could include redistributing other authorities' cyber security advice. AEMO could use their existing Market Notices system to share relevant information with market participants, or another means.

Question 9: Do you consider the benefits of claryfing the facilitating the distribution of cyber security information to market participants as a function in the rules outweigh the costs/risks? Why/why not?

4 Making our decision

When considering a rule change proposal, the Commission considers a range of factors.

This chapter outlines:

- issues the Commission must take into account
- the proposed assessment framework
- decisions the Commission can make.

We would like your feedback on the proposed assessment framework.

4.1 The Commission must act in the long-term interests of consumers

The Commission is bound by the National Electricity Law (NEL) to only make a rule if it is satisfied that the rule will, or is likely to, contribute to the achievement of the national electricity objective.[28]

The NEO is:[29]

> to promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to—
>
> (a) price, quality, safety, reliability and security of supply of electricity; and
>
> (b) the reliability, safety and security of the national electricity system; and
>
> (c) the achievement of targets set by a participating jurisdiction—
>
> (i) for reducing Australia's greenhouse gas emissions; or
>
> (ii) that are likely to contribute to reducing Australia's greenhouse gas emissions.

The targets statement, available on the AEMC website, lists the emissions reduction targets to be considered, as a minimum, in having regard to the NEO.[30]

4.2 We propose to assess the rule change using these four criteria

4.2.1 Our regulatory impact analysis methodology

Considering the NEO and the issues raised in the rule change request, the Commission proposes to assess this rule change request against the set of criteria outlined below. These assessment criteria reflect the key potential impacts — costs and benefits — of the rule change request. We consider these impacts within the framework of the NEO.

The Commission's regulatory impact analysis may use qualitative and/or quantitative methodologies. The depth of analysis will be commensurate with the potential impacts of the proposed rule change. We may refine the regulatory impact analysis methodology as this rule change progresses, including in response to stakeholder submissions.

Consistent with good regulatory practice, we also assess other viable policy options — including not making the proposed rule (a business-as-usual scenario) and making a more preferable rule — using the same set of assessment criteria and impact analysis methodology where feasible.

28 Section 88 of the NEL.
29 Section 7 of the NEL.
30 Section 32A(5) of the NEL.

4.2.2 Assessment criteria and rationale

The proposed assessment criteria and rationale for each is as follows:

- **Safety, security and reliability**

We selected security, safety and reliability because safety and security outcomes for consumers are the end goal of the proposed rule change. Cyber security incidents present an energy sector risk that could have significant consumer impacts. The rule change request sets out that the current ad hoc nature of AEMO's cyber security activities and lack of dedicated funding poses an ongoing security risk to the NEM. The proposal seeks to create a formal cyber security role for AEMO, which could help enable the secure provision of electricity to end customers over the long term. This assessment criterion will be used to assess how any changes made to AEMO's cyber security role and responsibilities will support AEMO's ability to manage and operate a secure system.

- **Principles of good regulatory practice**

The issues in this proposed rule change request relate to the problem of the rules not being fit for purpose by not specifically identifying AEMO's role and responsibilities in relation to cyber security. Principles of good regulatory practice will be critical to selecting the best solution for this rule change request. The proposed solution seeks to promote predictability and stability in cyber security (for the electricity industry) by placing more well-defined responsibilities on AEMO.

The rule change request seeks to improve transparency around AEMO's cyber security role for all stakeholders including governments and industry. Simplicity in implementing the rule change will help to minimise the administrative burden on AEMO and reduce costs for industry participants. The rule change proposal also aims to outline principles and key functions without being overly prescriptive.

This assessment criterion will be used to assess how any changes made to the rules enable AEMO to play a clear role in cyber security, without unduly limiting AEMO's cyber security work, nor placing new obligations on other industry participants. It will also assess how the design of the solution needs to consider this broader direction of reform to leverage other cyber security initiatives and avoid duplication.

- **Implementation considerations**

Implementation considerations will be critical to considering a solution for this rule change request. This assessment criterion will be used to assess the cost of the proposed solution, both directly and indirectly.

It will also assess whether now is the right tie for the rule change based on the expected costs and benefits (see chapter 3 for more information on the expected costs). Relevant factors will include the level of cyber security risk and interactions with other reforms, including outside the AEMC.

Although the rule change focuses on AEMO's responsibilities, all industry participants have a role to play in cyber security. In addition, there are cyber security risks to businesses in the electricity as well as end-use customers. Therefore, impact analysis for all stakeholders will be key to the rule change process.

This assessment criterion will also focus on whether the proposed solution is a market-wide solution that is effective for all NEM jurisdictions. This is especially true given that cyber security risks are not necessarily tied to a physical location. We will consider both federal cyber security initiatives as well as any jurisdictional differences.

Question 10: Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?

4.3 We have three options when making our decision

After using the assessment framework to consider the rule change request, the Commission may decide:

- to make the rule as proposed by the proponent[31]
- to make a rule that is different to the proposed rule (a more preferable rule), as discussed below, or
- not to make a rule.

The Commission may make a more preferable rule (which may be materially different to the proposed rule) if it is satisfied that, having regard to the issue or issues raised in the rule change request, the more preferable rule is likely to better contribute to the achievement of the NEO.[32]

4.4 The proposed rule would not apply in the Northern Territory

Parts of the NER, as amended from time to time, apply in the Northern Territory, subject to modifications set out in regulations made under the Northern Territory legislation adopting the NEL.[33]

The proposed rule would not apply in the Northern Territory, as it amends provisions in NER chapter 4 that does not apply in the Northern Territory.[34] Consequently, the Commission will not assess the proposed rule against additional elements required by the Northern Territory legislation.

31 The proponent sets out its proposed rule in Attachment A of the rule change request, pp. 11 - 13.

32 Section 91A of the NEL.

33 National Electricity (Northern Territory) (National Uniform Legislation) Act 2015 (**NT Act**). The regulations under the NT Act are the National Electricity (Northern Territory) (National Uniform Legislation) (Modification) Regulations 2016.

34 Under the NT Act and its regulations, only certain parts of the NER have been adopted in the Northern Territory. The version of the NER that applies in the Northern Territory is available on the AEMC website at: https://energy-rules.aemc.gov.au/ntner.

Abbreviations and defined terms

5MS	Five-minute settlement
ACSC	Australian Cyber Security Centre
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
AESCSIRP	Australian Energy Sector Cyber Security Incident Response Plan
CER	Consumer Energy Resources
Commission	See AEMC
DER	Distributed Energy Resources
NEL	National Electricity Law
NEM	National Electricity Market
NEO	National Electricity Objective
NER	National Electricity Rules
NGL	National Gas Law
NGO	National Gas Objective
NGR	National Gas Rules
NTP	National transmission planning
Proponent	The proponent of the rule change request
SRA	Settlements Residue Auction